that is not expired, lost or stolen. It also verifies the individual's identity and that he or she is not wanted, barred or suspended from entering the installation, and has access to the installation under the Force Protection Condition.

If a restriction has been placed on the individual, the screen display will tell the guard how to proceed. "DBIDS virtually eliminates the threat of unauthorized persons gaining access; stopping them at the front door so to speak," McGee said. "And these operations not only act as a physical protection measure but also as a deterrent."

The screen displays include color photo, identity information, color-coded message screens, audible sounds to quickly and easily alert the guard of the individual's status and a variety of administrator capabilities. In addition, the text on the screens is multilingual. "All this occurs in a matter of two to three seconds of the scan, less time than it takes the guard to visually validate an ID card," McGee said.

The scalable system can cover a building, installation or entire theater of operations.The majority of DBIDS sites, including CFAY, use fingerprint scans when the FPCON or installation policy dictates that additional checks are required. However, DBIDS Kuwait uses hand geometry because of the difficulty encountered in trying to capture usable fingerprints from laborers.

At CFAY, DBIDS equipment was deployed in 2004 with the opening of a registration center. In April, gate access and the Visitor Control Center were installed. Nearly 32,000 people are registered at CFAY in DBIDS and approximately 22 percent are DBIDS cardholders. The remainder are DoD identification cardholders, according to McGee.

Fully operational DBIDS installations include: U.S. Armed Forces Europe; U.S. Armed Force Korea; Fort Hood, Texas; Fort Polk, La.; Monterey Peninsula, Calif.; and U.S. Joint Task Force, Southwest Asia (Kuwait and Qatar).

DBIDS expansion is an ongoing process throughout many areas of the DoD. This expansion has led to the creation of the new Identity Authentication Office within DMDC, which is dedicated to managing DBIDS. In addition to working on improved versions of the system, the office is investigating linking to other government identity authentication systems to share data and digital fingerprints using CAC chips for authentication.

New DBIDS deployments are underway at Yokota Air Base in Japan and other areas in Southwest Asia, according to McGee.

For more information about DBIDS, please visit the DBIDS Web site at https://www.dmdc.osd.mil/dbids/.

Michele Buisch is a contractor supporting the Department of the Navy Chief Information Officer. CHIPS

Implementation of PKI Authentication for DADMS

The use of the Public Key Infrastructure (PKI) and the Common Access Card (CAC) for accessing the Department of the Navy Applications and Database Management System (DADMS) became mandatory Sept. 6, 2005, according to a coordinated naval message: AL NAVADMIN (UC) R 012042Z SEP 05 issued by the Department of the Navy Chief Information Officer (DON CIO) and the Assistant Chief of Naval Operations for Information Technology (ACNO-IT).

This action is being taken to provide additional assurance that only personnel authorized by the current DADMS access control process have access to the network and application information contained in DADMS.

DADMS users must either have a valid PKI software certification (softcert) installed on their system or use a CAC reader and software to provide the authentication.

DADMS users are advised that PKI softcerts have an expiration date at which time the softcert will become invalid. Softcerts are no longer being issued. Once the softcert expires users will be required to use their CAC for authentication.

Navy Marine Corps Intranet (NMCI) desktop computers or laptops are provided with a CAC reader and ActivCard Gold software required for authentication purposes. In addition to the CAC and ActivCard Gold software, users must enter their individual personal identification number (PIN) code which they created when their CAC was issued.

Users accessing DADMS from non-NMCI computers must have a CAC reader attached to their computer as a peripheral and have the ActivCard Gold PKI Common Access Card software installed to provide the authentication.

PKI authentication is in addition to the user identification (ID) and password currently required to log onto DADMS. PKI authentication does not change the current method of obtaining access to DADMS. Any DADMS user ID and password problems should still be reported to the DADMS help desk. CAC problems are to be reported to command CAC issuing activities since the DADMS help desk cannot assist with CAC problems.

Use of the CAC to access DADMS can be tested immediately and is encouraged to ensure CAC problems have been addressed.

For additional information contact the ACNO-IT at (703) 604-7813. CHIPS